ICANN82 | CF – GNSO: BC Membership Work Session
Tuesday, March 11, 2025 – 10:30 to 12:00 PST

BRENDA BREWER

This session will now begin. Please start the recording.

Hello and welcome to the business constituency membership work session on 11 March 2025 at ICANN82, Seattle. My name is Brenda and I am the participation manager for this session. Please note this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Antiharassment policy. If you would like to speak during this session please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute in Zoom. Online participants will use a physical microphone to speak. Please state your name for the record and speak at a reasonable pace, and I will now hand the floor over to BC chair Mason Cole.

MASON COLE

Brenda. Good morning everybody. Welcome to the BC in person meeting here in Seattle at ICANN82. Good to have everybody in the room and we have some remote participants as well. We have an hour and a half together today, and our agenda is on the screen. If you would also, and I have to do it, log into the Zoom room, that's how we'll manage the queue today please, so please do that, take care of that chore.

Are there any updates or additions to the agenda please?

CHING CHIAO Mason, I'd just to—

MASON COLE Ching.

CHING CHIAO Sorry, thank you Mason. I have one item on the AOB. I'd just like to remind you.

MASON COLE Okay, thank you Ching.

CHING CHIAO Thank you.

MASON COLE Great, okay. All right, so we have two guest presentations today. First is from Mark Robertshaw who we heard from in Istanbul with an update on the DNS Research Federations work on the impact of the RA and RAA amendments that came into effect last April. This is relevant to our ongoing concerns about DNS abuse and then we'll have a brief presentation from Ching and Ed from WhoisXML API on abuse tactics, and then Segunfunmi, who is remote, is going to do a policy calendar review and then we'll cover AOB. If there's anything else that needs to be added to the agenda please raise

your hand right now. Otherwise we're going to five right in. Okay. Mark, are you on screen and ready?

MARK ROBERTSHAW I am indeed. Thank you Mason.

MASON COLE All right, the floor is yours. Welcome to the BC.

MARK ROBERTSHAW Thank you very much. It's really good to be with you again following my first visit in Istanbul and to be able to provide and update on the work we've been doing on tracking mitigation rates following the RAA changes. Next slide please.

Many of you will have come across this before, but those that haven't, we are a not-for-profit entity based in the UK and our general mission is to advance understanding of the DNS impact on cybersecurity policy and technical standards and that's largely involved in education and research, access data and engagement in technical standards. Thank you, next slide.

This is our roadmap for today. We're going to talk a bit about the project again to recap on that, talk again about methodology, but a bit more in brief this time, provide you with an update on the findings since we last spoke in November, and also provide you with some idea of a comparison with other studies that have come out recently which you may have become aware of, too, about the

differences in results that we may have experienced there, and also to then talk about the next steps. Thank you, next slide.

Just to set the scene, this will be very familiar to all of you by now I hope and expect. What we're looking at here are the key changes to the RA that have come into effect over the last, I guess coming up to a year or so now, which have tightened the definition of what DNS abuse actually means, called out explicitly malware, botnets, phishing, pharming and spam when it serves as a delivery mechanism for other forms of abuse, but also the point that's under the new RAA registrars must promptly take appropriate mitigation action. We also refer to the existing provision 318.3, which was already in the RA previous to the amendments, which talks about that illegal activity submitted to contacts must be reviewed within 24 hours by an individual empowered by registrars to take action. Those are the key bits of the RA we're looking at today for this study. Next slide please.

Our objectives are that for all applicable abuse reports we're measuring how much mitigation is being detected, how quickly it's happening and by which parties. Of course, for the purpose of today our studies very much focus on the contracted parties here, registrars and registries, and to effectively monitor the trends over time of the effectiveness of the amendments on the speed and rate of mitigation. Next slide please.

Recapping on our methodology, we did this in quite come detail last time, so I'm not going to do this in multiple slides today, we'll just take you through the highlights. What we do effectively is we

start with phishing and malware reports obtained from those third part sources you see on the screen there. These are reports that have been sent, we've received from those third parties reported typically by people that have experienced abuse. We then duplicate those reports and record the unique domains that we find on a daily basis. We then go through a process of removing subdomain providers and URL shorteners using a list that's compiled by Korlabs and that effectively means that we're looking at malicious domains rather than compromised domains in general because we believe those are the domains that we think registrars and registries can effectively take action upon as opposed to compromised domains, which are much harder and much more downstream and there what we do is we check each domain for a mitigation. Immediately when we see the report, at zero days, and at one day, three days, seven days, 14, 30, 90 and finally a year. Once we've seen a mitigation we then stop and record the mitigation time at that point. Next slide please.

To be clear, what we're measuring here are mitigations that we believe the contracted parties can actually do effectively and we're not looking at downstream mitigations at this stage. We're looking at just the things that we believe can be attributed directly to registrars and registries, and for registrars that really is applying a client hold status to the domain of the registry, deleting the domain effectively, which often pushes it into the RGP, redemption grace period, and sometimes the domain will pass the expiry date and sometimes that's recorded as a mitigation as well. For registries it's very clear, really just a server hold is the operation that the registry

can operate and we've been very clear that we're just measuring these very key actions that can be affected by registrars and registries to very definitely mitigate abuse and stop the domain from rooting at that point. We're being really clear that no downstream mitigation is being measured at this stage. We're not measuring hosting provided mitigations. We're not measuring things like reverse proxies and registrants. We're just looking at these very clear mitigations that can be affected by the contracted parties at this stage.

MASON COLE: Mark, I'm sorry to interrupt. Would you take questions as you go, or would you prefer to wait until the end?

MARK ROBERTSHAW: Of course. Very happy to take questions as I go. Are there some coming aleady?

MASON COLE: Yeah, Steve has one in the queue. Steve, would you like to ask?

STEVE DELBIANCO: Hey Mark. Just wanted to know, which of the mitigation steps you've listed here, which you talk about them as being high confidence, which of them prevent a victim from having a bad domain result? In other words, which of them stop people from being victimized?

MARK ROBERTSHAW They all stop the domain. They're very strong mitigations, all of these. There's no possible that the domain will root after applying these actions, to be clear.

STEVE DELBIANCO Thank you Mark.

MASON COLE Crystal has a question.

CRYSTAL ANDO Thanks Mason, Crystal Ando **[? 8:40]**, Google. Does domain past expiry date, does that not include deletions that happen during AGP?

MARK ROBERTSHAW It can do, indeed, yes, that's right. It's the other type. RGP is typically what we normally see. There's also some very interesting patterns where occasionally domains will be used at the very end of their lifecycle for abuse purposes and then will actually expire, which typically then results in a mitigation, and that will often be applied by the registrar, usually by policy, to the disable the domain in some way, but it can be arduous, and you're quite right, the AGP process is also a reason for that. But we're looking at things basically where the domain will no longer be rooting at this point.

CRYSTAL ANDO Sorry, just to be clear, because a majority, not majority, a very large portion of malicious registrations are done and caught by registrars within the five-day period and they like to get their money back from registries, so they delete them within five days. Are we not capturing or considering that as mitigation of these?

MARK ROBERTSHAW Yes, that would be caught as a kind of RGP abuse type.

CRYSTAL ANDO Got it, thank you.

MARK ROBERTSHAW It would be caught under that one there. Yeah, absolutely. Yeah. Any more questions before we move on?

MASON COLE No, go ahead Mark.

MARK ROBERTSHAW Next slide please. Okay. Now we'll move on to the updates on the findings we've got so far to date. Next slide please Brenda. Just in terms of background we started collecting data in September 2024 and the last time we reported we showed you a fairly, two- or three-months' worth of data, so we've now been collecting for a longer period of time. The focus today is very much on 24-hour

mitigations, and the reason is this is the only timeframe that's mentioned in the RAA and also frankly reflects the short timeframes of many phishing and other malicious activities. We are very much focusing in on the time that's the critical period for mitigation to take effect. As we've mentioned already, all reports are based on number of maliciously registered unique domains observed daily for all received reports, and what that means for us is that when we're looking at monthly aggregations of numbers we're not counting domains uniquely within a month but we're counting domains daily and summing those up to get a monthly total, and the reasoning behind this is that what it gives us is the ability to capture where perhaps an abuse report has come in, say on the first of the month, no action has been taken. Coming on the fifth of the month for the same domain no action was taken, comes again maybe on the 20th of the month and then action is taken, we want to reflect that there were previous reports that weren't acted upon as well as recording of course the final report. What we're doing here is we're choosing a granularity that best reflects that 24-hour period and counting things multiple times if indeed they do present a problem and are not mitigated throughout the month. That gives you a sense of the reason why we count in this way.

Moving onto the next slide please. This is a chart of date and 24-hour mitigation rates that we're observing collectively for registries and registrars between the time we've been monitoring and you can see by this chart, the best fit line there, that we are seeing a general upward trend in mitigation. When we start monitoring we're typically seeing rates around the 10 or 12 percent of domain

reports daily being mitigated within 24 hours. Now we're seeing on the order of roundabout, on average, 20 percent. We're seeing a definite improvement over this period in the numbers, the amount of mitigation happening within 24 hours, which is encouraging. Next slide please.

In terms of the mitigation action taken by actors, this is a very interesting comparison because this shows us how fast things are happening but also who's doing what, when. You can see that we have an average mitigation time actually across all the registrars and registries. Registrars are about, almost eight days actually is the average mitigation time that we see. For registries it's about, just under seven days, just over seven days. But what you'll see, it's interesting here that within 24 hours we see more action, typically, by registries and only when we get to about seven days beyond that point do we start to see more action being taken by registrars. Whilst we don't expect registries to take that much action typically what we're seeing is that the split is that registries are taken action faster in the first 24 hours and it's taken longer typically for registrars to take that action. Next slide please.

Now, this is a quite complicated chart to explain, so I'll try and explain this carefully. What we're saying here is that in the ideal, this is a breakdown of the numbers of registrars that we're seeing with different mitigation rates. Taking all the registrars that we've observed over the whole period, what percentage are we seeing with only a 10 percent mitigation rate within 24 hours? That's the big slice of the pie on the lefthand side, and then the next size pie would be those that we're seeing up to 20 percent within 24 hours.

The ideal solution, outcome here would be that the whole chart was a light green color. That would be the ideal, where 100 percent of registrars are mitigating within 24 hours or below, but actually what we're seeing at the moment is a much, much smaller pinch, and actually three quarters of registrars are only mitigating up to 20 percent within 24 hours. Obviously the seven-day pitch for comparison on the right gives a slightly better picture and that reflects very much what we described in the previous slide, that typically registrars are acting, if they're acting, they're acting somewhat slower than 24 hours, but the stats do improve when you extend the time period to seven days. We get a more broad reach, but still very little. The more than 40 percent light green mitigation rate is a very small percentage of registrars that are actually mitigating at that level even after seven days. Next slide please.

This is the comparative registry focus here. What we have here is the breakdown for registries and as we've already described we wouldn't expect registries to be taking as much action as registrars, and in fact the stats are slightly worst in terms of the numbers of registries that are taking action within 24 hours, but you can see that the past improves at seven days as well. That gives you a sense of the breakdown. The main key message here is that we're not seeing very much activity at 24 hours. Certainly not rates of more than 40 percent mitigation. Next slide please.

This gives you the long term and also gives you a sense of the spread here. This is looking at all of the mitigations that we've seen for combining registries and registrars over the period, and it

shows you the percentages. Of course, these figures are cumulative, so by the time we get to 30 days we're typically seeing 35 percent mitigation rates, but you can see that as we go down in time back down to the 24 hours, we're seeing typically this 15 to 20 percent over the period and a sweet spot forming around about the seven-day mark. Again, that gives you a sense of the spread where if there's action going to be taken by registries and registrars, it's likely to be more around the seven-day mark than around the 24-hour period, which is the key period we believe for consumers to be affected by abuse. The next slide, please.

In terms of the key takeaways from this presentation I suppose are that there's slight improvements in mitigation rates but the pace is too slow. If we extrapolate out those figures it would take us probably to at least 2030-ish to see 100 percent mitigation rates in 24 hours, if we carried on the trend we are at the moment. We're not seeing enough pace in terms of improvement in mitigation rates. We believe that contracted parties need better tools, access to intel and also an ability to report back as well, and we're involved in a number of initiatives as an organization which are looking to provide better tools to registrars, but we do believe that it's possible for this gap to be closed if contracted parties have the tools they need to receive the information in a timely way to be able to act upon it. I was very encouraged earlier on today as it happens where a large registrar who was communicating to me that they are already taking these kinds of steps to get this intel from fee providers, to get engaged with those that have got the intel and are starting to take automated action in a very rapid way and trying to

reduce that gap. Because if we're going to actually have an impact on the consumer and stop that abuse within a 24-hour window we do need to give the registrars and the registries the tools they need to actually access that data in a way that's cost effective for them as well, within their profit margins, and a way that's going to work. I think the final point, just to make into the key takeaways, is there is an incomplete picture. We don't have the whole data set for the whole world yet as we're engaged in a large global project where we're collecting large amounts of data. We will be expecting higher volumes of data to come over the next few months and we hope to better have a bigger picture of a more global sense of how much abuse there is and how much mitigation is happening.

We're also just as interested in mitigations at the downstream level and in terms of hosting providers. That needs a different treatment to domain names, also. Just important to look at and then to start to consider things like compromised domains in the mixture as well. Any questions before I move on? I'm aware that I've spoken for a long time. Any hands up?

MASON COLE Thank Mark. I'll put my hand up first and then we'll go to the queue. You mentioned that there are opportunities for better tools for registrars. Would that include things like better response times, the ability to act at scale? These are some of the things the CSG is putting forward in terms of the contract amendments that we're advocating for next. Or not?

MARK ROBERTSHAW

Absolutely, and I think what we're talking about is a real time low latency access to data. One of the challenges has been that with the recent ICANN tooling for reporting abuse, it's been much too slow in terms of getting the data to the registrars, that sort of solution. What we really need here is automated systems that ingest data in almost real time and provide feeds back out to the registrars in almost real time, and we're looking at latencies of minutes rather than days or weeks, so that those registrars can realistically then take action in either an automated way or in a very responsive way on the data.

MASON COLE

All right, very good. I'll just remind the BC that the CSG has a session with the board at 4:30 today and this is undoubtedly going to come up, so I encourage you to attend that discussion. Crystal.

CRYSTAL ANDO

Thanks Mason. Crystal with Google. Just going back to the fact that you focused on 24 hours, I think everyone agrees that's a great milestone to hit. It would be amazing if we could take all bad domains down within the first day as a registrar. I don't own a registrar anymore, so this is in my BC capacity. I wanted to point out that you said 24 hours is the only time mentioned in the RAA. That's true, but it's only for law enforcement and government officials, not for other reports, so while you can hope and think that the amendments actually have anything to do with that provision,

they're completely separate from it. Registrars are required to intake from government, law enforcement, and respond within 24 hours. That's not the same requirement for DNS abuse. If you bring it to the board just be aware that that is a distinction. I would hate for it to say, "Oh, the amendments require 24 hours," because that's not what it is.

MASON COLE: Thanks for pointing that out, Crystal. Good point. Mark.

MARK ROBERTSHAW: Thanks Crystal for that, and I'll take that one on the chin happily and say that's fair enough. I think the main point for us is actually that the 24-hour window is the window in which most of the abuse is executed on the consumer and that's why the 24-hour window is so important for this process, if I can respond on that. Yeah.

MASON COLE: All right, thank you Mark. Other questions for Mark, please. Yeah, Nenad.

NENAD ORLIC: Have you ever in your monitoring reports, have you ever considered locality of the domains in terms of how does locality, in terms of both from where the abuse is coming from or where it is intended? Let me explain. For example, there is a website I discovered, it's still up, that's been known for the last three weeks in Serbia on an info domain that's been reported to all the certs, all

the official things, that represents itself as a payment service and I see three weeks later it's still up. What I'm saying is have you ever checked, does the locality of the abuse in terms of this is an abuse site intended for Serbian citizens? It's for the Serbian market, so how does locality of the abuse affect both takedown and also time to note it? Have you ever considered something like that?

MARK ROBERTSHAW That's a really good question and actually one of the things that we do with all of the reports that we receive from all of the providers that we mentioned is a whole process of enrichment of that data at the point that we receive it. We look up all manner of things, including the locality of the hosting provider for that report as well as the locality of the registrant if it's for the country within RDAP, if we can obtain that. We have that data to hand and actually whilst in this study we haven't focused on that at this stage, one of the outputs that we're producing as an organization as league tables focused on different strata of the, segments of the abuse chain. One of those things which we're hitting on quite soon is geography and we're focusing a lot on country-based league tables soon. We're hoping to have more on that for you I think in the future. Thanks for the question.

MASON COLE Good question, Nenad. Thank you. Chris.

CHRIS MONDINI Hey Mark. How are you doing?

MARK ROBERTSHAW Good thank you. How are you?

CHRIS MONDINI Yeah, really good, thanks. Just one question. I know you have a lot of data and I know we need to catch up on that because we haven't spoken for a little while, but no, I agree. It's really important to act as quickly as possible from once the abuse is live, but I wonder if you have any data on is there a period between a registration being live and then actually abuse being deployed to that domain?

MARK ROBERTSHAW Yes, that's a really good question. Actually, one of the challenges of looking at domain registrations is of course that many domains can sit there for quite some time before they're actively used and that's actually often one of the tricks of the scammers, is to register things and let them sit for a while so they look benign and then suddenly do something with them at a later point in time. We do have the states. We haven't analyzed those stats, though we do have that data, which is an interesting one for us to look at. The other thing that's probably more significant than domain registration time is data obtained from passive DNS sources, which people on the call may be aware of, which is a better indication of when something actually becomes live on the internet as opposed to is registered for theoretical use later.

That's my response. Chris, go ahead.

CHRIS MONDINI Yeah, sorry, one clarifying point. With the way that you're recording the time for action, is that based off of first seen of that abuse report or it time that domain has been live for, maybe with or without content?

MARK ROBERTSHAW We're looking at the reported dates, which is often a reported date that's passed on to us from the fee provider. It is, of course, impossible to know when the abuse started because there'll be a period of time between when… I won't say impossible. As mentioned, you can use passive DNS to work out when a phishing site when live, but when somebody actually started using… I think those are the measures you can use. You can use, as you say, created date is one measure. Passive DNS is another measure for first seen on the internet, but the measure that we can use practically is the reported date that's passed on because that's the earliest date that we have access to somebody reporting a problem with it. We appreciate that's not tight enough as a 24 hours, when we'd love to augment that with data we get from passive sources to make that even tighter.

MASON COLE Thank you for the quesitoj, Chris. Mark, Margie put a question in the chat about availability of your findings online. Are they available?

MARK ROBERTSHAW They will be. In fact what we're doing is this is a precursor to a published report which will be coming out by the end of April. That will be published at that point. This is just the findings which will be bootstrapping that report.

MASON COLE All right, very good. Other questions for Mark, please. Crystal.

CRYSTAL ANDO Thanks Mason. Will your methodology be fully transparent and published in that as well, or just the outcomes?

MARK ROBERTSHAW One hundred percent, absolutely, and that's something that we're committed to doing is being very transparent with our methodology and I think if it's helpful I can continue, if there's time, Mason, I can continue to talk about a comparison of our methodology with another study which you may have come across recently and to explain the differences, because actually one of the things that we're very clear about is that we want to be transparent. We also want to measure things in a way that's sensible given that we're focusing on these short timeframes as well, so absolutely. 100 percent.

MASON COLE: All right. Other questions for Mark, please. All right, Mark, looks like the queue is clear. Thank you for your presentation and for the information. Very helpful to the BC and its efforts, and we'll excuse you. You're welcome to stay, but you don't need to. We're going to proceed with the meeting and thank you for being here with the BC today.

MARK ROBERTSHAW: Thank you very much. It's been a pleasure. Thanks a lot.

MASON COLE: Okay, thank you. All right, we are going to move to the next agenda item, which is a brief presentation from Ching and Ed. Gentlemen, the floor is yours. Please, go ahead.

ED GIBBS: Oh, there we go. I have with me Alex Ronquillo as well, vice president of product at Whois API. I think this is my third or fourth time presenting at the BC. Yeah, and my job now is I got a little title change, vice president of research and I make sure that all this data that we collect, similar to what Mark does, we analyze it, we go through it and we produce these reports. I'm often asked from an engineering perspective because I have an engineering background, what does the data actually look like? What's behind the scenes? What I wanted to do is take a brief look into what that looks like and some of the data that we have so you can begin to

see what we see and how that interprets into some of these numbers that we talked about. Next slide please.

One of the things that I've heard since I've been here is, is bulk registration bad? Well, it can be, but not necessarily. There are different purposes and everything from testing, and I'll get into some of the things that we've seen conducted by some of these bulk registered domains, but they're not all malicious. A lot of them are preemptive or brand registrations and things. There's many, many reasons why people do this. I just want to make that clear, that we didn't necessarily focus on just malicious domains. We could have. I think there's a lot of people out there that are doing exactly that and there's no shortage of data or analysis that you can turn to read about malicious domains, but let's take just a general step back and see what we have to deal with here. Next slide.

Over the last three or four years, I could've gone back 14 years but what I wanted to do was take a look at what does domain clustering looking like? When I say clustering, these are bulk registrations that in these bulk registrations the names are very similar and we were using machine language on the back end to look for associations, and you might be familiar with the Levenshtein distance algorithm or FuzzyWuzzy. They've got all these different things out there that you can measure distance to what names look like, and then you've got the people out there that take seed values and you're starting with a known word perhaps, say for example Microsoft or Google, and then you're measuring the distance of these domain names to those to see if there's any relationship. Well, the challenge was about four years ago we changed all that. We got rid of seed values

completely and now we're using machine language in combination with some of our newer AI technology to identify what these clusters look like, so these spikes when you see 10,000, 14,000 domain names registered in a single day, that's because they're related in some way, somehow, using no inputs or parameters that would indicate any type of relationship, but having it figure out intelligently what these associations are.

It's interesting to see a lot of the TLDs being abused, particularly when some of the interesting ones, everything from dot motorcycles to dot boat to XYZ to top. Whatever the TLD is these people are registering massive amounts of bulk domains and we're able to correlate that and produce this chart. But you can see these spikes. The spikes are really interesting because they're repetitive, and further analysis, they show that, I don't want to say they're state sponsored, but some of them do appear very, very suspicious and so using some of the technology that we have we're able to determine even where these bulk registrations came from. I can't go into too much detail, but I do work a lot with the government agencies, so we did some further research, but these bulk registrations are becoming a problem. They have been a problem and they continue every single day. It doesn't take a break. Tomorrow there'll be hundreds of thousands more and everything from three on up to, like I said, you'll see 14,000, nearly 14,000 domains registered by a single entity. Next slide.

By the way, if you have any questions during the presentation let me know. I have Alex here as well to help me. He has a lot of exposure in this area, but when we look at domain clustering,

again, when it comes to malicious actors this is what they do. They'll register these various domains. They look like DGA, if you're familiar with DGA, these domain generate algorithms. They produce numbers and letters that make no sense to anyone and they'll register 500 to 1,000, whatever that number is. They know that a certain amount of those will get caught. What they do is they wait three months like we talked about, and six months later, whatever that timeframe is, they'll check back and see which ones were caught. The ones that weren't caught, they may weaponize those at that point. By weapon…

Yeah, generally the explanation of why they were caught, we don't necessarily get that information but they were caught nonetheless and various engines out there detected them. We ran some analysis against some of the major security providers out there to see how they classified those and it was quite revealing and very sporadic on what they were able to identify, but everything from phishing, brand impersonation, traffic distribution systems. How many people have heard of that? TDS. Yeah, this is fascinating because it's up-and-coming, so it's no longer, "Hey, I'll just register a domain, I'll use it for phishing, then go away." Now what they're doing is they're registering these groups of domains, these domain clusters and they'll bounce around even between non-distinct clusters and everything, these redirects are quite complex. They'll do 307, 308 to 302 to 301, and along the way, at each step of the way they'll identify what device you're coming from, your geo, browser characteristics. Is it real? Then ultimately you land at the destination and at that point they have some assurance that it is a

legitimate person making the request. If anything looks suspicious along the way in TDS they'll stop the traffic and it looks like you just hit a black hole. TDS, expect to see a lot more of that. Ad fraud, nothing new there, but in order to do TDS one of the things that really struck us is passive DNS. Mark talked about this a little bit. Give you last seen. Okay, that's great. Gives you the IP address resolution, which is wonderful, but what it's on a CDN or hosted cloud provider like Cloudflare or something? Then you reach a dead end. We had to have something more to pivot on, so we gained access to similar and additional information that allowed us to look at the distribution of traffic and identify what is TDS, including first access to these traffic distribution systems, because very often it requires a lot of testing and like I said, it's very complex. These people know exactly what they're doing. They're very technical, so it's kind of a game changer on that front. Like I said, using AI we're able to apply a lot of that to vast amounts of historical data and get away from the predefined keywords and start using trending methods and different ways of identifying these domains. Next slide.

So the homoglyph attacks are still out there. We see those a lot. Single domain names are difficult, kind of like the lone wolf because all it really takes in one domain to carry out any type of attach or anything, but for the most part the clustering with typo squatting is more prevalent. Like I said, when we look at Fuzzy matching, Levenshtein, these are great but you got to have a lot of resources to do that, especially when you don't even know what you're looking for. That's where it becomes a lot more complicated,

so the more GPUs you've got, the better. Being able to identify those, and like I said, those domains in these clusters, they remain in hiatus. We've seen some recently in hiatus for three years and all of a sudden become active. Those are very, very easy to identify based on some behavioral patterns that we can isolate and identify when they go active, so when we looked at research, okay. Do we identify a malicious domain one, three, five, seven, 30 days, 45 days out? We've got to go way beyond that because these domains that they're going after, they were registered before. They went into hiatus. They sit there for a very, very long time, sometimes years, and then they become active again. Being able to detect that first time activity is consuming, not on resources to do that, but the compute power, the algorithms to do that are very complex. That's where we spent a lot of time developing this. Go ahead. Next slide.

Like I said, leveraging AI really, if you're like me you see AI every day and you go, "Oh, not again." What's new and what's fake? It takes an incredible amount of talent to… Let me predicate this. AI is only as good as the people that write it, or can work with it, and we've hired some of those people that are very brilliant and can work with us in bringing AI to the forefront because it is very useful. It's extremely fast when properly deployed and can identify things that we had no idea we wanted to identify, so we're seeing a lot of that. Next slide.

Here's an example of a simple cluster. AI safety workshop day, registered across three TLDs. When we look at what was used we used a VirusTotal, OpenDNS and a few other products. Nothing identified it as suspicious. Now, when you look at the records, sure,

they're privacy shielded, maybe for a good reason. Who knows? Could be somebody working out of their house hoping to do some safety word ops and things. We simply don't know at this point, but we were able to identify that is is a cluster registered across different domains and using the same name servers. Next slide.

Here's a little bit more. You can see here that there is a cluster of 10 in the top TLD and we used VirusTotal, OpenDNS and Cloudflare to see if anything detected it as possibly malicious and VirusTotal was the only one. Now, that's the count of how many engines in VirusTotal detected it, so when it says two, one, one, that's out of 94 security products. That's a major… Is this bad? What is it? You can see at the time when I ran this analysis, 60 percent of the domain registrations in that cluster were missed, 100 percent across all security stacks. At some point even though they weren't active I expect those to be used and the trick is being able to capture that when they are used for the first time. Go ahead, next slide.

I did have the firewall vendor up. I took it out. I didn't want to pick on one single company, but you can see here that there were nine domains associated with Meduza Stealer in those IOCs and five domains could be found in the cluster that were not identified. It's great we caught the others, but what about the other ones that didn't get caught? Those remain out there and will probably be used at some point. Then again, they may never be used. We simply don/t know. Having that vague analysis of this is really what we have to work with today. We don't know. We could probably have these taken down, but what are they? It was an interesting

observation and these were 43 days earlier than reported that still nothing identified. Next slide.

Everybody likes to pick on Microsoft because it's one of the bigger scams out there. Microsoft tech support, Microsoft product, everything. We see this constantly, on a daily basis, Microsoft, and 1,660 bulk registered domains on February 8, a lot of those disappeared. I imagine the registrar took those down, but some of them remain. I'm not sure what this slide is, but again, we see these constantly on a daily basis. Next slide.

So, this is just some of the JSON output where we see the brand clustering, what was caught and what was missed. When I looked at those last night, that's still the case. The ones that were missed, it's unfortunate they're still around, but having the technology to identify those and feed that back to the community is really what we focus on and bring value back to that so that we can help protect the consumer. Go ahead, next slide.

Oh, LinkedIn is another one. Yeah, basically Microsoft again.

UNIDENTIFIED SPEAKER That's Cole, from Microsoft.

ED GIBBS Oh, I'm sorry.

COLE QUINN I like to think of ourselves as attractive.

ED GIBBS Very true, but as a top product in the industry, right, you're a target.

STEVE DELBIANCO It's obvious that keeping an updated blacklist is not going to keep up with the cleverness that employed with the registrations and you've given seven slides about innovations that you are perfecting with respect to technology and either a firewall or registrar. I hope you're giving this presentation to the registrars and resellers and registries while you're here in Seattle. Have they shown interest at licensing or using your services to improve their own screening?

ALEX RONQUILLO Yeah, I can speak to that a little bit. Again, Alex here, head of product. We serve a lot of the registrar community. Actually, some of the folks in this room as well and in many cases I think everyone is putting a lot of effort into trying to not have to deal with fraud and abuse things as early as possible, but the inability of any single registrar to see all of the global registrations, even in different CCTLDs, areas that are traditionally hard to see what domains exist, that sort of thing, we have a lot of the registrar abuse teams working with us very actively. In some cases even just profile and when they say people signing up through domains they may want to see, hey, has this person spun up domains in other places?

Right. Right, exactly. Right. But I think a lot of the content here is a larger point of us trying to figure out, hey, if it's clear one actor registered three, five, 10, 5,000 domains like we've seen in

Conficker malware, different types of attacks like that, is it okay for all of that other set to be innocent until proven guilty or should we be trying to put some effort into clustering those together even if they're using Italy, France, dotcom, dotnet, dot shop, all of that stuff at the same time. A lot of I think the work we do with registrars is focused on trying to sus out particularly stuff that registrar can't see that's out there in the world to try to get better predictive signals, maybe hopefully deal with that in that 24-hour period. We also work a lot with the cybersecurity vendor community, so a lot of the people in brand protection who do takedowns once this stuff has already been abused, a lot of them are using our past DNS to try to enrich those investigations, try to get ahead of this and even all the way down to the firewall vendors and the email security software of the world. They're also all trying to fight this same fight. I think some of the work we want to do here is, to your point, try to help the registrars a little bit to the left of the attack timeline, try to figure out what is going to be a problem or what has already been registered that's likely a problem.

STEVE DELBIANCO One tiny follow-up before Crystal. Is it clear that the registrars, registries, firewall providers, email providers have sufficient market demand for your services without having to be pushed into it by say an ICANN compliance measure.

ALEX RONQUILLO I think so, and that's a nice position for us because I think a lot of the firewall vendors are competing with each other trying to have

them out innovate each other. Same thing with the brand protection spaces, et cetera. I think everyone is trying to get to that as fast as possible. Can we also be the first ones there and then can we write our software as a way that they got to that answer faster?

CRYSTAL ANDO

I love that discussion and actually Steve I think you kind of hit it on the nose there. This is happening with the decent, good, reasonable registrars, however you want to call it, already, and I think tying back to the conversation we had with the CPH… Was that yesterday? I already forget what day it was. Sunday. Ones who aren't doing this work it won't matter if it's in the contract or not. They're not doing it already. If you put it in the contract it give ICANN something to terminate them with. You see that happening now already under the amendments as they're drafted. I think that's the problem a lot of us in the industry are coming towards, doing the right things and trying their best to learn how to level up. I think it's in everyone's best interest to get rid of abuse, but how do we find and give ICANN the tools to take down the ones who aren't here? I think that's where the next round of amendments, something like this would come into play.

ED GIBBS

Next slide. Pay toll, was it texting? I don't know how many of you have ever gotten a text message saying, "Hey, you haven't paid your toll." I live in Florida, and everything's a toll road in Florida. When these show up just about everybody I know has gotten these, but this is a really good example here where 18 percent of the

domain registrations in this cluster were identified or basically 100 percent of them were identified in the top TLD. Being able to identify that, this was caught by our AI engine almost immediately as soon as we saw them, because it began to build a pattern her and look at them. Sometimes we'll see thousands of these, particularly in the latest pay toll scams where this is becoming really popular, but you can see here the security vendors caught it. We ran it by some of the other security products out there, they also caught it. It is getting better, to some extent. Yeah, there's a couple of companies out there that are working with the cellular providers and things, but they're very…

Yeah. They're almost scared to block in a sense because they don't know what's legitimate and what's not, but I think it's become clear that if this becomes a repeated pattern, then it's safe to say there's no legitimate purpose for this. Next slide.

Just another one. This was caught. I'm not sure what this is, but it must mean something to somebody, whether it's DGA or something, or maybe it was brand registration. It's hard to say. It just doesn't make sense. We weren't able to identify what this was but again, the security products did a good job in identifying this cluster. Next slide.

CRYSTAL ANDO Sorry, I'm just going to jump in since you chose dot top. They have received a breach notice. I put it in chat, and one of the reasons why

ICANN specifically notes is failure to abide by the new DNS abuse obligations. The registry.

ED GIBBS: Right, registry law. Thank you for clarifying.

ALEX RONQUILLO: Sorry, one thing to note here also is there may be a discernible brand name in there. I can't find it myself necessarily but a lot of times when we're looking at these larger lists and there's a lot of detections like this, and especially when those detections come from VirusTotal, great product, a lot of times that's malware related. A lot of times these domains were used for command and control, attackers sending commands to a botnet or maybe exfiltrating data, but in these cases I think again, the larger point stands. Can we find these grouping faster, and how do we discern those groupings from, let's say an actual minerals company, maybe, that wanted to register 20 domains for different purposes or defensive purposes. Luckily for us, usually when it looks like crazy jargon statistically a lot of times that stuff ends up being either command and control malware domains. In some cases they're what Ed alluded to earlier, traffic distribution systems. Renee Burton over at Infoblox has done some very awesome work on traffic distribution systems, and again, that's a lot of what we see when we look at those inane looking domain names that have a clear… These aren't all targeting a LinkedIn dash login or anything like that.

ED GIBBS

What we don't see here is what's to the left of that, the subdomains, and that's really where passive DNS comes in handy or zone files, different things that could potentially be used with these for various purposes. Next slide. Oh, go ahead.

NENAD ORLIC

This strikes me as different from previous examples because previous examples were maybe visible abuse potential and such things, but there were so many misses in terms of detecting it as abuse. Here it's critical and it's 100 percent detected as abuse, so it's an anomaly in my opinion compared to the previous examples. Do you have data or opinion what made 100 percent identification possible in this cluster?

ED GIBBS

I think there was a particular bias that is being introduced into detection based on the TLD, the quality of the registrar, those weights being applied. Yeah, and there's a discussion I had last month with the forum. Should the top domain be blocked in an enterprise environment by firewalls and things? There are certain TLDs like XYZ, what legitimate purpose would someone have to get XYZ?

CRYSTAL ANDO

I'll just say Google uses abc.xyz as its main investor website, so that might just be one.

ED GIBBS That's true. Never heard of Google. But when it comes to these TLDs I think people are trying to figure out, can we blanket some rules or something and apply them and see what we can get away with? If there's legitimate cause we'll make an exception.

MASON COLE All right, gents. Just a quick time warning.

ED GIBBS Yep, all right. I think that was the last one. This one real quick7, rapid WHOIS record changes. This is interesting because I just happened to pick a day where I thought, let's see who's making WHOIS record changes or the most frequent and there was a TLD over in Europe that had a runaway script that made 300 changes over I think three months, so I picked that up, but I also in the process caught some interesting records where a group out of India were changing their records almost two or three times a day and misrepresenting themselves as big pharma. Not sure why they were doing it or who they were trying to impress. Doesn't matter. But it was interesting to see that there were those rapid changes taking place and we were able to catch that.

I think that's pretty much it. The next slide is just the conclusion. Like I said, detection's getting better. Better at threat detection. We've taken a more comprehensive multilayer approach and

reducing false positives. Although they do remain a concern, we're seeing those reduced.

MASON COLE: All right, Ed, Alex, thank you very much. Very interesting. Yes, go ahead Vivek.

VIVEK GOYAL: Thank you. Excellent presentation. Can you please let me know about that pharma in India? I'll see if I can reach out to the pharma and fix things, but I have two points to discuss here. A lot of reporting of what is a threat or not and these feeds that are used by different companies to do it are restricted to a geography where there has been threat and they are set up in that country or that region to set up, but countries like India where this thing is emerging, there are no companies providing feeds, so since nobody has it, nobody detects it, and that's why nobody has it. That is one problem that I don't know how to suggest to solve it.

The second point is anybody's knowledge about brands is based on your exposure to that region or to the brands that you know. What you might thing is a random string might be a big brand in some country you've never visited.

The third challenge is IDNs. I haven't come across anybody who was done significant work to see IDNs are either doing great or they are being used absolutely for malicious things, and I think from regions where you do not get these feeds, that's where there are multiple languages, where people are pushing, governments are

pushing for local languages to be used. That's where IDNs should be flourishing and why not for abuse? Anything you can share on this will be helpful. Thanks.

ED GIBBS

Yeah, yeah, yeah, that's a fantastic point. I think one of the main reasons that everyone from, particularly let's say the reactive side of the community, so brand protection all the way out through firewalls, trying to stop the connections going through those places, honestly, in many cases they probably can't see all the domains in dot-in, so there's no way for them to predict, let's say, what is going to be malicious. That's where we do a lot of our combining of things like certificate feeds to passive DNS to try to get a sense of, even if we can't see everything in dot-in, what can we see? How long has it been around? Is there any registration data to pull? There isn't always and if not that, can we get a sense, profile the hosting provider, those types of things? To your point I think the IDN problem is very pronounced, especially in specific regions and it gets complicated even further because when a lot of the brand protection companies are trying to figure out what they need to stop in those areas, to your point there may not be a great brand protection presence in India already. Already they lose the local context and that type of stuff.

There's a lot of these IDNs I think that translate out into the XN Punycode variance to try to resolve those non-English characters and then that makes it even harder for a brand protection company. Right, they're using seed values, they have permutations

already. They're looking for certain things but they may have been looking for paypal-login.xyz with a Spanish A, but were they looking for xn-p, xn-2452 something, whatever, aypal, and those types of things? On our site we do actually look at all of the domains that have any types of Punycodes and then try to translate them out. We also provide some early phishing warning signals to different brand protection firms highlighting that and we even go as far as translating out that Punycode back to what it looked like in that string. Yeah, again, coming back, I really think the visibility is probably the hardest piece. There's a lot of really good teams trying to study everything and trying to see what do I need to take down on behalf of my customers brand protection wise. Even they can't take down what they can't say.

VIVEK GOYAL Thank you. I am a brand protection company in India. I might not be great, but I'm pretty good. I'm trying my best.

ED GIBBS Hey, that's fantastic.

MASON COLE All right. Thanks for the question, Vivek. Any other questions for Ed, Alex, Ching? All right gentlemen, thank you very much. Good presentation. Appreciate your time with the BC today. Thank you.

All right, it's move on, on our agenda please. Segunfunmi, are you online?

SEGUNFUNMI OLAJIDE Yes, Mason, I'm here.

MASON COLE Good. We miss having you here, but you now have the floor. We just need a quick highlighted overview of the policy calendar please.

SEGUNFUNMI OLAJIDE Okay. Greetings to every one of you from the beautiful city of Abuja, Nigeria. I was really looking forward to being in Seattle in person, but unfortunately my US application process took way longer and that is why I'm unable to come in person, but today I'll be coordinating the policy calendar virtually and I look forward to an insightful discussion with every one of you.

I'll make an attempt to share my screen. Just confirm if you can see my screen clearly from your end.

MASON COLE We do see it.

SEGUNFUNMI OLAJIDE Okay, great. All right, on the channel one of our BC policy calendar we've not filed any public comments since the last time that we met, so moving on to open public comments. We currently have one open public comment which is on the fourth proceeding of the proposed language of the draft session of next round AGB. On this particular one there are several areas of concern or areas worth

noting to BC membership in drafting this comment. That is the application fee, name collision and brand eligibility requirement and several others as listed in the document. On this we have three volunteers already from the BC. Thanks to Ching Chiao, Vivek Goyal and Asteway Negash for volunteering to draft a BC comment. This is also still open because this comment closes on the second of April. If there be anyone within the BC willing to contribute to this comment, kindly indicate so that your name can be included in the drafting team.

Moving onto channel two, which is council activities and previous council meeting. The previous council meeting was held on 15th of February and also attached in this policy calendar is the agenda and the recordings for the BC meeting, for the council meeting. Also, the next council meeting will be on the 12th of March, 2025, at 5:00 UTC and at this point I should be turning it to our councilors, Vivek or Lawrence to guide us through what we should be expecting in the next council meeting and then what positions the BC is looking at taking or what direction the BC is looking at taking in the next council meeting. Let me know who wants to go first, Vivek or Lawrence.

LAWRENCE OLAWALE-ROBERTS: Good day all. This is Lawrence. I will start off and Vivek will follow. We have a council meeting slated for tomorrow and top of the agenda starts with a concept agenda. We now have a small, statutory small team called SCCI, who's responsibility it is to take on special tasks for the council. It's not just comprised of

councilors. It also has community members across the different constituencies within the GNSO. They had their first meeting at this particular, a few days back. We will be confirming Manju as the chair for this particular committee.

Of interest to the BC will be the second item where we vote, is about the new candidates, or rather the appointed candidate for board seat 13, which is for the contracted party house. Greg DiBiase of Amazon will be stepping into that role come AGM and I believe that that will be when Becky Burr, who currently has that seat will be stepping down from the ICANN board.

Right after that it was supposed to be, we're also going to be voting on the transfer policy. We've had subsequent discussions, meetings prior to now and everything seemed to be going well and hopefully will go well but just recently, yesterday I guess, a group within the council brought up what we call a condition that the transfer policy should undergo a CPI, GPI, should be tested for GPI, the global public interest framework and human rights framework. Based on this there were proposals to basically, since this is completed we are to vote on this and pass it onto the board for their decision and probably some implementation thereafter. The thought is that since the framework didn't kick in in the life of the working group, that the framework should be passed to the chair of the working group to assess the work of the working group for the global public interest and rights and if there is anything flagged they will be doing this work alongside, they will be doing that assessment alongside the NCUC, I guess, and if there is anything flagged for human rights they brought that to the attention of

council and probably now advise the board after we have moved this onto the board. I don't know if we have any questions before, or any reactions before Vivek takes on the others.

ZAK MUSCOVITCH: Thank you Lawrence. Zak Muscovitch. That's news to me. I participated in that transfer policy working group for a good four years and no one has raised that framework previously, so I'm a little surprised that now that the final report is completed it's being raised. Thank you.

LAWRENCE OLAWALE-ROBERTS: That was also, it also came as a shocker to a number of us on council. It was interesting because the position of the council before we now are adopting this new position was to still pass on the transfer policy as is to the board and the NCUC, who were interested in this, could now advise council… Sorry, could now advise the board after they do their own assessment. It was thought to be a bad precedent because not only would we have one constituency within the GNSO speaking to the board directly on issues that concern the entire GNSO, but the framework was put together after the life of this particular working group, so for the locked and dyed critics for instance, we understand that the framework has been passed to them, but one interesting also that staff shared with us was that these are obligatory conditions. In other words, I feel, my own personal thinking in my personal

capacity, I feel that the working group could also decide if they would like to implement or not implement.

SEGUNFUNMI OLAJIDE: Okay. Thank you for that insightful commentary on that.

LAWRENCE OLAWALE-ROBERTS: Sorry. I understand Steve has a question for me.

SEGUNFUNMI OLAJIDE: Okay, yeah, great. Steve DelBianco, please go ahead.

STEVE DELBIANCO: Thanks Segun. With respect to the two GNSO board seats that you discussed earlier, the BC has for a decade advocated GNSO have four board seats, not two, so that we wouldn't have to take turns or take prisoners with the NCPH, with the NCSG. My question is did the contract parties and Crystal and others, did the contract parties struggle with figuring out who their next board seat would be given that they have both registrars and registries, and isn't this an opportunity to show that it only makes sense that there be four, not two from the GNSO?

CRYSTAL ANDO: I can't give you all the special sauce and whatever. I don't think it's public. That said, we vote in the BC, so we did not participate in the CPH vote, but it was a brand-new process coming out of this year.

Historically I think it was known as registries take a turn and then registrars take a turn. That era is over. There's a formalized process. It went to multiple votes across all houses. It took months. It was complicated. I think we got to the right place. I'm really excited for Greg to step in but it was a very formalized process that both parties agreed to before we entered into it.

VIVEK GOYAL

Thank you Lawrence. Thank you for the comments. Zak and others, don't worry. We'll try our best to get this thing approved without it being stuck with something. We were as pissed as you are when this thing happened. I'm going to talk about next steps on registration data accuracy. For those who attended the GNSO council meeting with GAC you would have remembered that this was a sticky point with the Europe and the Indian members. They said we have been waiting for you to come back on this quite some time, but the next steps in the GNSO council is that the report is being prepared where all the comments from different constituencies are being put together and will be up for discussion the next meeting. Nothing major has happened on this yet.

On the other hand, major things have happened on the billing contact. For some members on the GNSO council this is a done thing. This should not be discussed. Billing contacts should be taken out because it has been discussed again and again and found to be irrelevant but we don't want a bad precedent to be set where an absence of direction on a topic should be considered as that it is taken out by default. Just because we're not seeing anything about

it, that means it's not relevant. Having had that discussion the leadership and council have come up with three options for this thing to go forward. One is a motion agreeing with the IRT determination but making it very clear that this will not serve as a precedent of superseding other contractual policy obligations. Basically coming up with the precedence that this will not set a precedent, which is again a precedent. I love council.

Second one is a new PDP on the subject, which raised so many voices in the council. We can't do PDP again on this. The third suggestion was acknowledgement that this work should be brought up in a subsequent PDP but suggesting a compliance deferral until this work is started, which seems to be a middle ground now on, fine, let's not take a call on this. Let the other work from the IRT go forward and be implemented and then when it's the right time we will put this into another PDP and get closure on this.

Again, we are suggesting this to the whole BC and based on your direction and the discussions here we will take this back to the council and take this forward. Personally, on a personal notion, I don't think allowing a precedent to be set where based on an absence of direction on something it should be taken that they didn't want to take it forward so they didn't talk about it. It should be said in any way possible. Thank you. I'll take any questions. Otherwise that's all on the council for now.

SEGUNFUNMI OLAJIDE Yes, Crystal. You can have the floor.

CRYSTAL ANDO Thanks. I don't see how this isn't dealt with now. I don't think the GNSO council should look that. Registries, registrars have already started moving to the new registration data policy set. That implementation has already been done. Just a reminder, the billing contact is not the credit card information. It is not the credit card holder. It's literally just a field that registrants can put whatever they want in there. It's not a used field. It has not been a useful field for decades. It's like removing fax machine requirement from our notice provisions. We're still working with ICANN to remove snail mail. They literally email me something, print it out and then mail it to me 47 times for each TLD. This was cleanup work. My understanding was it was discussed during this work, during the temp spec. It was discussed again with registration data policy. I just think taking the position that it needs to be waiting until the next PDP is non-tenable for us. I get the principle, but there has to be a way to actually go forward. I don't see the win here other than the precedent issue. You're not actually asking for billing contact to continue to be collected, right? That's not the ask. Or is that the ask from the BC?

SEGUNFUNMI OLAJIDE Vivek, please go ahead with a final comment.

VIVEK GOYAL

What has happened is during this discussion in the GNSO council we have heard that billing contact is used in other places which may not be as evident to us, and I'm not challenging the validity of the data in that contact because I personally register domains. I just copy paste the whole thing across all. For example, if a registrar fails and this data, and all the information is given to a new registrar, they do not have the actual billing contact that the registrar maintains, like the credit card information. They are supposed to use the billing contact to reach the registrant. They are supposed to. Crystal, I agree with you. If there's no data in it you can't do anything, but because there was no clear direction it cannot be determined that they went through all those impact analyses and then decided that, so our focus is more on the precedent for this than whether it is useful or not and again, we will go as the BC says. We will put our voice forward.

CRYSTAL ANDO

Just to be a little bit more precise here, when you transfer a domain you have to give your credit card information to the gaining registrar. They have that because you have to buy a new year during that transfer. So again, the billing contact is a little appendage that no one really cares about and hasn't looked at for years, so I just don't want the BC to be seen as preventing a very useful change or clarity in something that really ultimately does not mean anything to us at the end of the day.

SEGUNFUNMI OLAJIDE Thank you for that insightful contribution. Margie, would you like to clarify or shed more light on the comment?

MARGIE MILAM Sure. This is Margie Milam in my personal capacity. I understand that billing contacts have been used for privacy proxy customers in the scenario that we were talking about, not necessarily new transfers, because that makes sense that the registrar would have to ask for the information, but where a registrar goes out of business that's where it might come into relevance. That's one area to keep in mind.

SEGUNFUNMI OLAJIDE All right. Thank you. I think the queue is clear. I would like to move to channel three, which is CSG activity and I would like to call on Marie Pattullo, if you have updates for the BC membership.

MARIE PATTULLO Sure. Hey, Segunfunmi, we miss you. Keep this nice and brief. Hopefully you've already been in all of the meetings I'm going to talk about. Non-contracted party house, one of the many things we discussed, Steve, was the four seats. Whether we'll get traction on that we don't know. We thought it was the time to actually raise it in a more formal settting.

The CSG meeting wasn't terribly dynamic. One of the main takeaways from that was Russ, who is not David Olive., he has taken over from David Olive, knows us, and he knows the contracted

parties very well. He doesn't know us very well and a theme, if you like, that the entire CSG is pushing at this meeting is, "Hello, we're the CSG," and knocking on people's foreheads trying to remind them that we exist, too, even though we don't have contracts.

The session on Sunday with the CPH, my personal takeaway was it was really good. There was no one shouting at each other. There was no blood. Nobody stormed out in a fit of pique. This is actually quite a big thing. Thank you. Massive thanks to those of you who presented, to Chris, to Vivek, to Cole. Yay team BC. We've got a few ideas as to how we're going to keep this going. We think it's important that we don't just have a meeting and then go away, that we actually try and take this forward and keep talking, keep discussing with each other. Finally, this afternoon you are all going. I know. I know you are because I'm going to check. You are all going to come to the CSG meeting with the board where Mr. Mason Cole, chair of the CSG, chair, looking happy, is going to… Exactly. Is going to lead us through some really fabulous subjects with the board and I'm going to hand over to you to talk about that, Mason.

MASON COLE Yeah, quickly, one of the questions that the board is asking every stakeholder group is about legislation outside of the ICANN sphere impacting DNS policy. Their specific question is how do we get governments to stop legislating around ICANN. It's a big question. It as big implications for ICANN. We have some thoughtful input

that we've worked out with the CSG. I'll be delivering that at 4:30 today.

MARIE PATTULLO: Back to you Segunfunmi.

SEGUNFUNMI OLAJIDE: All right, thank you. Thank you for those contributions. Just before I turn it back to Mason I would like to ask, will there be any questions or contributions for our councilors before they proceed to the next council meeting? I'm looking for hands or comments. Okay, in the absence of no other questions or contributions, Mason, I'll turn this back to you. Thank you.

MASON COLE: Thank you very much Segunfunmi, and we look forward to having you in person in Prague. Hope that your visa issues are resolved well in advance of the Prague meeting. All right. Let's move to AOB. Ching, please.

CHING CHIAO: Thank you Mason. Actually this is for the NomCom, for the 2025 NomCom. I think, do you want to say, or… Okay. We put a short announcement on the submission portal about the geographic calculation for the board seat as we just discussed about that. The cc and Gs, they have North American board directors. One has already sitting in and one is to be seated, so that means that for this year the selection cycle, North American candidates for the board

will not be considered, the candidates from North America. However, we put an announcement out there so, because this is still before the deadline, so if that can be cured, if you or if you know anyone who has already submitted, then that can be also cured. Please email to the NomCom staff and we will let you know how that can be done, if the options are available to you.

MASON COLE To move to another continent?

CHING CHIAO There will be a statement out there to see how that can be cured, once again, if that option is available. Then obviously there's future cycles or other leadership positions that you can apply, but one last thing on this one is that the system is relatively new so you don't want to be in the last minute to submit the specific… The system, you need to have an ICANN account and then use that as a single login method to login to the application portal. Don't wait to the last minute and then if something went wrong. Just want to put it out there. Thank you very much.

MASON COLE Thank you Ching. Arinola, anything to add?

ARINOLA AKINYEMI No, I think that Ching did a good job.

MASON COLE Zak, please.

ZAK MUSCOVITCH Thank you. Zak Muscovitch. I'm putting to the chat a link to the 25th anniversary of the UDRP conference, which has been convened by WIPO in Geneva the end of April. Some people you may know are participating. For example, Paul McGrady, Lori Schulman and myself will be leading a panel on UDRP review and so you're all welcome to join in person, but if not, it's also available online as well. Thank you.

MASON COLE Thanks for that heads up Zak. Very useful. All right. We are almost at time. Is there any other business for the BC today? All right, very good. Thanks everybody. Thanks Brenda for he support. BC is adjourned.

BRENDA BREWER You may stop the recording. Awesome job everybody.

[END OF TRANSCRIPTION]